SSA-654382: Vulnerabilities in SIMATIC S7-1200 CPU Familiy

Publication Date:	2014-03-20
Last Update:	2020-02-10
Current Version:	V1.3
CVSS v3.1 Base Score:	8.8

SUMMARY

The latest product release of the SIMATIC S7-1200 CPU fixes several vulnerabilities. The most severe of these vulnerabilities could allow an attacker to take over an authenticated web session if the session token can be predicted. The attacker must have network access to the device to exploit this vulnerability.

Further vulnerabilities resolved in this product release are discussed below.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): V2.X and V3.x	Update to V4.0 http://support.automation.siemens.com/WW/view/en/86567043

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Products of the SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2014-2249

The web server of the affected PLCs (port 80/tcp and port 443/tcp) might allow CSRF (Cross-Site Request Forgery) attacks, compromising integrity and availability of the affected device.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2014-2258

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 443/tcp (HTTPS). A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2250

Due to low entropy in its random number generator, the integrated web server's authentication method (port 80/tcp and port 443/tcp) could allow attackers to hijack web sessions over the network if the session token can be predicted.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-332: Insufficient Entropy in PRNG

Vulnerability CVE-2014-2252

An attacker could cause the device to go into defect mode if specially crafted PROFINET packets are sent to the device. A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2254

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 80/tcp (HTTP). A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2014-2256

An attacker could cause the device to go into defect mode if specially crafted packets are sent to port 102/tcp (ISO-TSAP). A cold restart is required to recover the system.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ralf Spenneberg from OpenSource Training for coordinated disclosure of CVE-2014-2258
- Alexander Timorin and Alexey Osipov from Positive Technologies for coordinated disclosure of CVE-2014-2250 and CVE-2014-2252
- Lucian Cojocar and Jonas Zaddach from EURECOM for coordinated disclosure of CVE-2014-2254
- Sascha Zinke from FU Berlin's work team SCADACS for coordinated disclosure of CVE-2014-2256
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2014-03-20):	Publication Date
V1.1 (2014-03-25):	Updated Section Acknowledgement
V1.2 (2014-04-15):	Updated Affected Products
V1.3 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.